

攻防世界Reverse进阶区-Guess-the-Number-writeup

原创

y4ung 于 2020-09-21 21:52:10 发布 372 收藏 1

分类专栏: [ctf](#) 文章标签: [ctf](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/qq_35056292/article/details/108720136

版权



[ctf 专栏收录该内容](#)

35 篇文章 0 订阅

订阅专栏

1. 介绍

本题是xctf攻防世界中Reverse的进阶区的题Guess-the-Number

题目来源: su-ctf-quals-2014

题目描述: 猜个数字然后找到flag.

2. 分析

文件下载下来是一个jar包。在 <http://java-decompiler.github.io/> 下载jd-gui, 下载下来双击运行即可, 免安装。

代码如下, 读取用户输入的数字保存到guess_number, 只有当my_number / 5 == guess_number时, 才会进入打印正确信息的if块, 跟进以后发现if块中的内容和guess_number毫无关系, 只是用来计算flag的。。因此最终guess_number应该为: `my_number / 5 = 309137378`, 命令行执行下面的命令, 得到flag: `a7b08c546302cc1fd2a4d48bf2bf2ddb`

```
$ java -jar 6a8bee79ee404194bb8a213a8a0e211d.jar 309137378
your flag is: a7b08c546302cc1fd2a4d48bf2bf2ddb
```

```

import java.math.BigInteger;
public class guess {
    static String XOR(String _str_one, String _str_two) {
        BigInteger i1 = new BigInteger(_str_one, 16);
        BigInteger i2 = new BigInteger(_str_two, 16);
        BigInteger res = i1.xor(i2);
        String result = res.toString(16);
        return result;
    }

    public static void main(String[] args) {
        int guess_number = 0;
        int my_num = 349763335;
        int my_number = 1545686892;
        int flag = 345736730;
        if (args.length > 0) {
            try {
                guess_number = Integer.parseInt(args[0]);
                if (my_number / 5 == guess_number) {
                    String str_one = "4b64ca12ace755516c178f72d05d7061";
                    String str_two = "ecd44646cfe5994eb35bf922e25dba";
                    my_num += flag;
                    String answer = XOR(str_one, str_two);
                    System.out.println("your flag is: " + answer);
                } else {
                    System.err.println("wrong guess!");
                    System.exit(1);
                }
            } catch (NumberFormatException e) {
                System.err.println("please enter an integer \nexample: java -jar guess 12");
                System.exit(1);
            }
        } else {
            System.err.println("wrong guess!");
            int num = 1000000;
            num++;
            System.exit(1);
        }
    }
}

```



[创作打卡挑战赛](#) >

赢取流量/现金/CSDN周边激励大奖